What is claimed is:

1. A method relating to probabilistic digital signatures of a message, between a signatory and a checker, using a probabilistic algorithm based on the calculation of a discrete logarithm, comprising the steps of:

for the signatory, generating at least two signatures $(r_1,s_1)$ and $(r_2,s_2)$ for the same unchopped message, said signatures being calculated by the algorithm by means of the same public and private key parameters using respectively distinct random values and, and

for the checker, checking all the signatures $(r_1,s_1)$ and $(r_2,s_2)$ of said message.

2. A method according to Claim 1, wherein the probabilistic algorithm is the Digital Signature Algorithm.

3. A method according to Claim 1, wherein the probabilistic algorithm is the Schnorr algorithm.

4. A protected device of the chip card type, having an electronic component that implements a signature method between a signatory and a checker, using a probabilistic algorithm based on the calculation of a discrete logarithm, that includes the steps of:

for the signatory, generating at least two signatures $(r_1,s_1)$ and $(r_2,s_2)$ for the same unchopped message, said signatures being calculated by the algorithm by means of the same public and private key parameters using respectively distinct random values and, and

for the checker, checking all the signatures $(r_1,s_1)$ and $(r_2,s_2)$ of said message.

5. A device according to Claim 4, wherein the electronic component is an 8-bit microcontroller.